UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/646,606	08/21/2003	Vincent J. Zimmer	42.P16845	9801

7590 12/21/2006

R. Alan Burnett
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

EXAMINER	
LOVING, JARIC E	
ART UNIT	**PAPER NUMBER**
2137	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	12/21/2006	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/646,606	ZIMMER ET AL.	
	Examiner	Art Unit	
	Jaric Loving	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 August 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 August 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 17-26 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. On page 25, paragraph [0074] of the specification, Applicant provides, "... a machine-readable medium may include propagated signals such as electrical... or other form of propagated signals (e.g., carrier waves, infrared signals...)." Therefore, the claims are non-statutory.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-4, 9-14, 16-18, 24-25, 27-28, and 30 are rejected under 35 U.S.C. 102(e) as being anticipated by Hind et al., US 6,976,163.

In claim 1, Hind discloses a method, comprising:

issuing, via a caller computer, a request to have a firmware service be performed via firmware on a remote computer (col. 6, lines 4-19 and lines 53-55)

authenticating the caller computer (col. 11, lines 8-11; col. 13, lines 39-56); and

performing the firmware service if the caller computer is authenticated, otherwise denying access to the firmware service (col. 13, lines 39-63).

In claim 2, Hind discloses the method of claim 1, further comprising initializing a listening mechanism on the remote computer to receive the request (col. 9, lines 37-52; col. 10, lines 8-24).

In claim 3, Hind discloses the method of claim 2, wherein the listening mechanism is interrupt-based, further comprising asserting an interrupt on a processor of the remote computer in response to receiving the request (col. 9, lines 37-52; col. 10, lines 8-24 – hardware latch can interrupt).

In claim 4, Hind discloses the method of claim 2, wherein the listening mechanism is polling-based, further comprising periodically polling a network interface of the remote computer to determine if the remote computer has received a request (col. 6, lines 4-19; col. 9, lines 37-52; col. 10, lines 8-24 – update capability of programmable memory is enabled and therefore would await an update signal from a caller computer).

In claim 9, Hind discloses the method of claim 1, further comprising:

issuing at least one authentication certificate to the remote computer, each of said at least one authentication certificate containing authentication information corresponding to a respective caller computer (col. 12, lines 12-29; col. 15, line 57 – col. 16, line 45);

receiving authentication credentials from a caller computer (col. 12, lines 12-29; col. 15, line 57 – col. 16, line 45);

authenticating the caller computer via the authentication credentials in view of a corresponding authentication certificate from among said at least one authentication certificate issued to the remote computer (col. 12, lines 12-29; col. 15, line 57 – col. 16, line 45).

In claim 10, Hind discloses the method of claim 9, further comprising determining if an authentication certificate corresponding to the caller computer has expired (col. 12, lines 45-56; col. 14, lines 40-54; col. 17, lines 25-31 – firmware release level in certificate would determine expiration).

In claim 11, Hind discloses the method of claim 9, further comprising determining if an authentication certificate corresponding to the caller computer has been revoked (col. 12, lines 45-56; col. 14, lines 40-54; col. 17, lines 25-31 – update flag set to "NO" indicates revocation).

In claim 12, Hind discloses the method of claim 1, further comprising authenticating the remote computer (col. 6, lines 4-19; col. 10, line 60 – col. 11, line 14; col. 12, line 45 – col. 13, line 12).

In claim 13, Hind discloses the method of claim 1, further comprising sending encrypted traffic relating to the firmware service request and results of the request between the caller computer and the remote computer (col. 12, lines 22-44; col. 13, line 39 – col. 14, line 39).

In claim 14, Hind discloses the method of claim 13, further comprising performing a cipher negotiation between the caller computer and the remote computer to agree

upon an encryption technique used to encrypt and decrypt the encrypted traffic (col. 10, line 60 – col. 11, line 14).

In claim 15, Hind discloses the method of claim 14, wherein the encryption technique employs at least one session key (col. 10, line 60 – col. 11, line 14; col. 11, lines 19-31 – special key).

In claim 16, Hind discloses the method of claim 1, wherein communications between the caller computer and the remote computer are performed using an out-of-band communication channel that operates independent of an operating system to run or running on the remote computer (col. 6, lines 4-19).

In claim 17, Hind discloses an article of manufacture, comprising:

a machine-readable medium on which a plurality of instructions are stored, which when executed perform operations comprising:

receive a request from a caller computer to perform a firmware service (col. 6, lines 4-19 and lines 53-55);

authenticate the caller computer (col. 11, lines 8-11; col. 13, lines 39-56); and

perform the firmware service if the caller computer is authenticated, otherwise denying access to the firmware service (col. 13, lines 39-63).

In claim 18, Hind discloses the article of manufacture of claim 17, wherein execution of the plurality of instructions further performs the operation of initializing a listening mechanism to receive the request (col. 9, lines 37-52; col. 10, lines 8-24).

In claim 24, Hind discloses the article of manufacture of claim 17, wherein the article comprises a firmware storage device and the plurality of instructions comprise firmware (col. 6, line 64 – col. 7, line 16).

In claim 25, Hind discloses the article of manufacture of claim 17, wherein execution of the plurality of instructions further performs the operation of performing a cipher negotiation between the caller computer and a remote computer on which the plurality of instructions are executed to agree upon an encryption technique to be used to encrypt and decrypt encrypted traffic to be sent between the caller computer and the remote computer (col. 10, line 60 – col. 11, line 14).

In claim 26, Hind discloses the article of manufacture of claim 25, wherein the encryption technique employs a shared asymmetric session key (col. 10, line 60 – col. 11, line 14; col. 11, lines 19-31).

In claim 27, Hind discloses a computer system, comprising:

a processor (col. 6, line 64 – col. 7, line 16);

a memory, operatively coupled to the processor (col. 6, line 64 – col. 7, line 16);

a network interface operatively coupled to the processor (col. 8, lines 8-20); and

at least one flash device operatively coupled to the processor on which firmware instructions are stored, which when executed by the processor perform operations comprising (col. 6, line 64 – col. 7, line 16; col. 8, lines 33-63):

receive a request to perform a firmware service received from a caller computer via the network interface (col. 6, lines 4-19 and lines 53-55);

authenticate the caller computer (col. 11, lines 8-11; col. 13, lines 39-56); and

perform the firmware service if the caller computer is authenticated, otherwise denying access to the firmware service (col. 13, lines 39-63)

In claim 28, Hind discloses the computer system of claim 27, wherein execution of the firmware instructions performs the further operation of periodically polling the network interface to determine if the network interface has received a request from a caller computer to perform a firmware service (col. 6, lines 4-19; col. 9, lines 37-52; col. 10, lines 8-24).

In claim 30, Hind discloses the computer system of claim 27, wherein execution of the firmware instructions further performs the operation of performing a cipher negotiation between the caller computer and the computer system to agree upon an encryption technique to be used to encrypt and decrypt encrypted traffic to be sent between the caller computer and the computer system (col. 10, line 60 – col. 11, line 14).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 5-8, 15, 19-23, 26, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind and further in view of Hsu, 2005/0081036.

In claim 5, Hind fails to disclose issuing an authentication challenge to the caller computer; and evaluating a response by the caller computer to the authentication

challenge. Hsu discloses issuing an authentication challenge to the caller computer (paragraphs [0039]-[0047]); and evaluating a response by the caller computer to the authentication challenge (paragraphs [0039]-[0047]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Hind's method of updating firmware with Hsu's key generation system utilizing an authentication challenge to use other encryption methods. It is for this reason that one of ordinary skill in the art would have been motivated to provide Hind's method of updating firmware with an authentication challenge because it minimizes the amount of traffic sent and increase the frequency of challenges (Hsu, paragraph [0033]).

In claim 6, Hind, as modified, discloses the method of claim 5, wherein the operations further include:

encrypting original data using a first key held by the remote computer to create encrypted original data (col. 10, lines 51-67; col. 14, lines 15-39);

sending the encrypted original data to the calling computer (col. 12, lines 12-63);

decrypting the encrypted original data using a second key held by the caller computer to create decrypted data (col. 6, lines 4-19; col. 12, lines 12-63);

sending the decrypted data back to the remote computer (col. 6, lines 4-19; col. 12, line 12 – col. 13, line 12);

comparing the decrypted data with the original data to authenticate the calling computer (col. 12, lines 34-36).

In claim 7, Hind, as modified, discloses the method of claim 6, further comprising extracting the first key from an authentication certificate for the caller computer issued to the remote computer (col. 13, lines 48-52).

In claim 8, Hind, as modified, discloses the method of claim 7, wherein the first key is an public key contained in the authentication certificate and the second key comprises a private key held by the calling computer that is the asymmetric key for the public key (col. 12, lines 22-32 and lines 56-63; col. 13, lines 48-52).

In claim 15, Hind fails to disclose the use of a session key. Hsu discloses employing a session key (paragraph [0044]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Hind's method of updating firmware with Hsu's key generation system utilizing a session key for encryption. It is for this reason that one of ordinary skill in the art would have been motivated to provide Hind's method of updating firmware with a session key because it helps protect traffic between network devices (Hsu, paragraph [0044]).

In claim 19, Hind fails to disclose issuing an authentication challenge to the caller computer; receiving a response to the authentication challenge from the caller computer; and evaluating a response by the caller computer to the authentication challenge. Hsu discloses issuing an authentication challenge to the caller computer (paragraphs [0039]-[0047]); receiving a response to the authentication challenge from the caller computer (paragraphs [0039]-[0047]); and evaluating a response by the caller computer to the authentication challenge (paragraphs [0039]-[0047]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Hind's method of updating firmware with Hsu's key generation system utilizing an authentication challenge to use other encryption methods. It is for this reason that one of ordinary skill in the art would have been motivated to provide Hind's method of updating firmware with an authentication challenge because it minimizes the amount of traffic sent and increase the frequency of challenges (Hsu, paragraph [0033]).

In claim 20, Hind, as modified, discloses the article of manufacture of claim 19, wherein evaluating the response to the authentication challenge comprises:

extracting authentication credentials for the caller computer contained in the response (Hsu, paragraphs [0043]-[0044]);

identifying an authentication certificate corresponding to the caller computer (Hind, col. 12, lines 12-29; col. 13, lines 39-56); and

checking authentication credentials for the caller computer against the authentication certificate that is identified (Hind, col. 12, lines 12-29; col. 13, lines 39-56).

In claim 21, Hind, as modified, discloses the article of manufacture of claim 20, wherein execution of the plurality of instructions further performs the operation of determining if the authentication certificate that is identified has expired (col. 12, lines 45-56; col. 14, lines 40-54; col. 17, lines 25-31).

In claim 22, Hind, as modified, discloses the article of manufacture of claim 20, wherein execution of the plurality of instructions further performs the operation of

determining if the authentication certificate that is identified has been revoked (col. 12, lines 45-56; col. 14, lines 40-54; col. 17, lines 25-31).

In claim 23, Hind, as modified, discloses the article of manufacture of claim 19, wherein execution of the plurality of instructions performs further operations including:

generating a random number (Hsu, paragraphs [0033], [0041], [0044]);

encrypting the random number using a first key to create an encrypted random number (Hsu, paragraph [0044]);

sending the encrypted random number to the calling computer (Hsu, paragraphs [0043]-[0044]);

receiving decrypted data derived from the encrypted random number from the calling computer (Hsu, paragraphs [0043]-[0044], [0053])

comparing the decrypted data with the random number to authenticate the calling computer (Hsu, paragraph [0041]).

In claim 26, Hind fails to disclose the use of a session key. Hsu discloses employing a session key (paragraph [0044]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Hind's method of updating firmware with Hsu's key generation system utilizing a session key for encryption. It is for this reason that one of ordinary skill in the art would have been motivated to provide Hind's method of updating firmware with a session key because it helps protect traffic between network devices (Hsu, paragraph [0044]).

In claim 29, Hind fails to disclose issuing an authentication challenge to the caller computer; receiving a response to the authentication challenge from the caller computer; and evaluating the response to determine whether the caller computer is authenticate. Hsu discloses issuing an authentication challenge to the caller computer (paragraphs [0039]-[0047]); receiving a response to the authentication challenge from the caller computer (paragraphs [0039]-[0047]); and evaluating the response to determine whether the caller computer is authenticate (paragraphs [0039]-[0047]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Hind's method of updating firmware with Hsu's key generation system utilizing an authentication challenge to use other encryption methods. It is for this reason that one of ordinary skill in the art would have been motivated to provide Hind's method of updating firmware with an authentication challenge because it minimizes the amount of traffic sent and increase the frequency of challenges (Hsu, paragraph [0033]).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: Frantz et al., US 7,085,385; Jorgensen et al., US 7,103,772; Cromer et al., US 6,684,326; Barr et al., US 6,189,100; Curry et al., US 6,105,013; Wang et al., US 6,199,194; Schmidt, US 5,826,015; England et al., US 2005/0144448; Zuccherato et al., US 2006/0095769; England et al., US 2005/0278531; Goh et al., US 2004/0010686; Tardo et al., US 2003/0226018; Palekar et al., US 2003/0226017; Kamperman, US 2002/0120847.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jaric Loving whose telephone number is (571) 272-1686. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JL

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER